REMARKS/ARGUMENTS

The courteous telephone interview granted applicants' undersigned attorney by Examiner Mark Afolabi on December 30, 2009 is hereby respectfully acknowledged. The arguments and amendments discussed in the interview are presented herein.

Claims 1, 10, 12, 15, and 18 are amended and claims 8 and 9 are canceled herein. With entry of this amendment, claims 1, 2, 4-7, 10-12, 15-18, and 20-23 will be pending.

Claims 1, 2, 4, 5, 7-11, 15-17 and 21-23 stand rejected under 35 U.S.C 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0257999 (MacIsaac), in view of U.S. Patent No. 7,047,316 (Iwata).

Claim 1 is directed to a method of estimating traffic values or intervals in a communications network. The network includes a plurality of nodes connected by links. The method includes obtaining traffic data through the nodes or links as input data, obtaining network data relating to the network topology and network behaviour, and estimating the effect of a modification of the communications network or its behaviour by calculating traffic information between a selected first and a selected second node of the network using the input data. Traffic data includes traffic measurements for said links obtained from one or more of the nodes in the network and that the network data includes end-to-end paths in the network.

Claim 1 has been amended to further include repeating step (c) for different pairs of first and second nodes corresponding to different modifications and selecting, according to predefined criteria, one or more candidates for modifying the communications network corresponding to one or more of the modifications.

MacIsaac is directed to detecting and disabling a source of network packet flooding. A packet flood detection device is interposed between a client computer and a server computer (Fig. 1). MacIsaac do not obtain traffic data including traffic measurements for links obtained from nodes in the network. Instead, MacIsaac collects data transmitted over a link. There is no traffic measurement for links which is obtained from nodes in the network. Instead, MacIsaac collects traffic data received on a single link

(e.g., link 7), which is connected to a network device in the network 1. The detector is thus positioned to receive only traffic data transmitted to client computer 4. (See, Fig. 1 and paragraphs [0040]-[0041].)

Furthermore, MacIsaac do not obtain network data relating to the network topology and network behaviour, wherein the network data includes end-to-end paths in the network. In rejecting the claims, the Examiner refers to paragraph [0090] of MacIsaac. This paragraph describes how a packet flooding detector receives data traffic information at a point in a network being monitored. Information is provided to a burstiness estimation mechanism and a utilization estimation mechanism. The packet flood detection device does not obtain network data relating to the network topology and network behaviour. Instead, MacIsaac simply looks at traffic received at the detection device to determine if packet flooding occurs. MacIsaac is only concerned with the traffic received at the detector and is not concerned with network topology.

With regard to the end-to-end paths, the Examiner refers to Fig. 1 of MacIsaac. The data collected is for a path from a client computer 4 to a network 1, which connects the computer 4 to other network devices (e.g., computers 2, 3). MacIsaac do not obtain network data comprising end-to-end paths. The end-to-end path in MacIsaac is from the computer 4 to a destination such as one of the computers 2, 3. Instead MacIsaac only looks at traffic at segment of a path. The end-to-end path would include the data links, routers, bridges, switches, hubs, etc. in the network 1.

Furthermore, MacIsaac do not disclose estimating the effect of a modification of the communications network or its behaviour by calculating traffic information between a selected first node and a selected second node of the network using the input data. The Examiner refers to paragraph [0046] with respect to this limitation. This section of the patent application describes how the detection device samples network traffic. The data is used to estimate a measure of the burstiness of the network traffic, which is used to determine whether packet flooding is occurring. There is no teaching of estimating the effect of a modification of a network or it is behaviour. As noted above, MacIsaac only looks at received traffic data. MacIsaac does not look at network topology or behavior thus the invention cannot be used to estimate the effect of a modification of the network.

As noted by the Examiner, MacIsaac does not teach obtaining traffic data through nodes or links as input data comprising traffic measurement for the links obtained from one or more of the nodes.

Iwata et al. describe link state routing techniques. A path is selected from a plurality of precalculated paths which are stored for each destination. The precalculated paths reflect link resource information. In contrast to Iwata et al., MacIsaac is concerned with analyzing data traffic associated with messages at a packet flooding detector to detect packet flooding at a specified location in the network. Iwata et al. use bandwidth information to select a path.

Neither MacIsaac nor Iwata et al., either alone or in combination, show or suggest estimating the effect of a modification of a communications network. Applicants' invention as set forth in the claims, is particularly advantageous in that is allows the impact of a modification to be estimated using the traffic data and network data from the initial, unmodified network in a relatively inexpensive way without the need to calculate traffic values using more complex models. This estimation may be used, for example, to automatically select certain modifications out of a set of possible modifications and to evaluate the impact of each modification. The best candidates for a proposed set of modifications can thus be determined and a more complex and complete analysis of these best candidates can then be performed.

Furthermore, the detector of MacIsaac is not located between different pairs of nodes, therefore, step (c) of claim 1 cannot be repeated for different pairs of nodes. Since MacIsaac does not estimate the effect of a modification of the network, there is no selecting a candidate for modifying the network, as required by amended claim 1.

Accordingly, claim 1 is submitted as patentable over MacIsaac.

Claims 2 and 4-11, depending either directly or indirectly from claim 1, are submitted as patentable for at least the same reasons as claim 1.

Claim 4 is further submitted as patentable over MacIsaac which does not disclose a modification comprising a modification of the network topology, a modified routing algorithm parameter, a modified traffic engineering constraint, or a modified traffic load.

As previously discussed, there is no estimation of an effect of a modification of a network. In rejecting the claim, the Examiner refers to paragraph [0077] of MacIsaac, which describes disabling a link in response to a packet flooding condition or other action taken in response to a packet flooding condition. These actions are taken in response to determining that a packet flooding condition exists on a link. These are not modifications for which an effect is estimated, as set forth in the claims.

With regard to claim 5, MacIsaac does not disclose detecting inconsistencies in input traffic data. Instead, MacIsaac simply discusses how traffic data may be corrected to include overhead associated with each packet.

Claim 7 is further submitted as patentable because, as previously discussed, MacIsaac does not evaluate the impact of network modifications.

Claims 15-18 are submitted as patentable for at least the reasons discussed above with respect to claim 1.

Claims 6, 12, 18, and 20 stand rejected under 35 U.S.C. 103 (a) as being unpatentable over MacIsaac in view of U.S. Patent Application Publication No. 2003/0058798 (Fielscher et al.).

The Fielscher et al. patent application is directed to approximation methods for finding minimum cost flows with shared recovery strategies. Fielscher et al. disclose a linear program that may be used to model how to route traffic.

As described above, MacIsaac do not disclose a traffic flow model for a network topology including end-to-end paths in the network as set forth in claims 12 and 18.

Furthermore, MacIsaac do not teach a plurality of constraints describing network topology and behavior as set forth in claim 12. In rejecting the claims, the Examiner refers to a packet filtering rule. The packet filtering rule is not a constraint describing network topology.

The cited references also do not show or suggest correcting input data if inconsistencies are detected, wherein correcting comprises using traffic data measurements and constraints describing network topology, as set forth in claim 12. In rejecting the

claims, the Examiner refers to col. 2, lines 15-35 of Iwata et al. This section of the Patent is the Background of the Invention, which describes drawbacks to precalculated path information. The Examiner also refers to paragraph [0052] of Fleisher et al., which describes a linear program that may be used to model how to route traffic in the Internet. The Examiner has failed to point to any teaching of correcting input data if inconsistencies are detected.

Claim 12 is further submitted as patentable over the cited references which do not teach a modification comprising a modification of the network topology, a modified routing algorithm parameter, a modified traffic engineering constraint, or a modified traffic load. As previously discussed, there is no estimation of an effect of a modification of a network. Paragraph [0077] of MacIsaac describes disabling a link in response to a packet flooding condition or other action taken in response to a packet flooding condition. These actions are taken in response to determining that a packet flooding condition exists on a link. These are not modifications for which an effect is estimated, as set forth in the claims.

Claim 18 is further submitted as patentable over the cited references which do not show or suggest automatically selecting a promising candidate for a network modification by calculating a cumulated flow using traffic and network data, wherein the candidates are selected according to predefined selection criteria. In rejecting the claim, the Examiner refers to claim 8 of Fielscher et al. Claim 8 specifies initializing primary and second flows for each link to least one predetermined value, selecting a commodity and routing a demand for the selected commodity. Rather than selecting a promising candidate for a network modification, Fielscher et al. select a commodity and route a demand through the network for the commodity. Instead of using a predefined selection criteria, Fielscher et al. use a predetermined value to initialize flows. The flows are not used as a selection criteria.

Accordingly, claims 12 and 18 are submitted as patentable over MacIsaac, Iwata et al., and Fielscher et al.

For the foregoing reasons, Applicant believes that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a telephone conference would in any way expedite the prosecution of the application, please do not hesitate to call the undersigned at (408) 399-5608.

Respectfully submitted,

Cindy S. Kaplan
Reg. No. 40,043

P.O. Box 2448
Saratoga, CA 95070
Tel: 408-399-5608
Fax: 408-399-5609